UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/635,015	08/04/2003	Christopher L. Hamlin	03-0340	7590

24319 7590 09/04/2008

LSI CORPORATION
1621 BARBER LANE
MS: D-105
MILPITAS, CA 95035

EXAMINER	
KHOSHNOODI, NADIA	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
09/04/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/635,015	HAMLIN, CHRISTOPHER L.	
	Examiner	Art Unit	
	NADIA KHOSHNOODI	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-14 and 16-22* is/are pending in the application.

4a) Of the above claim(s) *23-31* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-14 and 16-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 August 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/17/2008 has been entered.

Response to Amendment

Claims 6 and 15 have been cancelled. Applicant's arguments/amendments with respect to pending claims 1-5, 7-14, and 16-22 filed 5/8/2008 have been fully considered, but they are not persuasive.

Response to Arguments

Applicants contend that Elazar et al. fail to teach "said buried nucleus including at least a matrix multiplier." Examiner respectfully disagrees. Elazar et al. teach that the DRM component, i.e. buried nucleus, contains a decrypting component (par. 33 and par. 39). Furthermore, Elazar et al. teach that several different types of encryption/decryption algorithms may be used in order to encipher/decipher the data, one of which includes AES (par. 35). Specifically, it is known in the art (and inherent to AES) that this particular encryption algorithm incorporates the use of a matrix multiplier. Thus, Elazar et al. teach that the DRM component contains a decrypting component and that AES may be used as the algorithm, hence Elazar et al.

teach that the buried nucleus includes at least one matrix multiplier even though the particular term "matrix multiplier" does not appear in the disclosure.

Due to the reasons stated above, the Examiner maintains rejections with respect to the pending claims. The prior arts of records taken singly and/or in combination teach the limitations that the Applicant suggests distinguish from the prior art. Therefore, it is the Examiner's conclusion that the pending claims are not patentably distinct or non-obvious over the prior art of record as presented.

Claim Rejections - 35 USC § 103

I. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 1-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elazar et al., US Pub. No. 2004/0039932, and further in view of Parks et al., US Patent No. 7,146,504.

As per claim 1:

Elazar et al. teach a distributed architecture of an information handling system, comprising: a buried nucleus inaccessible for inspection without heroic means while said buried nucleus is in operation (par. 26 and par. 30), said buried nucleus including at least one matrix multiplier (par. 33, par. 35, and par. 39); and a trusted authority for generating a secure protocol, said secure protocol controlling operation of said buried nucleus (par. 33), wherein authorization information is securely conveyed into the buried nucleus via the secure protocol, thereby causing

the buried nucleus to operate and return a result, the result utilizable for activating an authorized operation (par. 38-39).

Not explicitly disclosed is wherein the authorization information being processed by the buried nucleus when the buried nucleus is in operation, thereby making said authorization information and information relating to processing of said authorization information inaccessible for inspection without heroic means once said authorization information is conveyed to the buried nucleus. However, Parks et al. teach that a license is securely provided to the trusted computer component and that the license must be evaluated, where the information is processed in a manner that allows the user to easily circumvent the system, thereby preventing the user to make alterations (col. 4, line 63 - col. 5, line 5). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Elazar et al. to process authorization information within the DRM component, i.e. buried nucleus, while it is in operation in order to render the information inaccessible to an attacker. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Parks et al. suggest that sending the content key in encrypted form secures the key so that only that specific user device can obtain access to the digital content the user is authorized to access in col. 4, line 50 – col. 5, line 17 and col. 5, lines 35-42.

As per claim 2:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one LFSR (linear

feedback shift register) (par. 25).

As per claim 3:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 1. Furthermore, Elazar teach wherein said buried nucleus includes at least one reconfigurable core (par. 27).

As per claim 4:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one programmable logic block (par. 27).

As per claim 5:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one non-volatile RAM (par. 27).

As per claim 6:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one matrix multiplier (par. 34).

As per claim 7:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said trusted authority is a back-end secure server (par. 33).

As per claim 8:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said trusted authority is a cell phone operator with a trusted command and control center (par. 29).

As per claim 9:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 1. Furthermore, Elazar et al. teach wherein said trusted authority is an encrypted medium (par. 33).

As per claim 10:

Elazar et al. substantially teach a distributed architecture of an information handling system, comprising: (a) a hardware/software system, comprising: a microchip including an outer region having I/O pins and a buried nucleus inaccessible for inspection without heroic means when said buried nucleus is in operation (par. 26 and par. 30, said buried nucleus including at least one matrix multiplier (par. 33, par. 35, and par. 39); and external software connected to said I/O pins for controlling said I/O pins (par. 25); and (b) a trusted authority for generating a secure protocol, said secure protocol controlling operation of said hardware/software system (par. 36); (c) wherein said buried nucleus is equipped to accept a key delivered through said secure protocol (par. 35, lines 15-16), wherein said key is conveyed into the buried nucleus via the secure protocol, thereby causing the buried nucleus to operate and return a result, the result utilizable for activating an authorized operation (par. 38-39).

Not explicitly disclosed is wherein the buried nucleus is equipped to securely convey an encrypted key, decipher an encrypted key delivered through said secure protocol, and wherein the encrypted key being deciphered within the buried nucleus when the buried nucleus is in operation, thereby making the deciphering operation inaccessible for inspection without heroic

means once said encrypted key is conveyed to the buried nucleus. However, Parks et al. teach that a trusted authority which supplies the protected digital content may also encrypt the key used to encrypt the digital content (col. 4, lines 59-61). Furthermore, Parks et al. teach that a license is securely provided to the trusted computer component and that the license must be evaluated, where the information is processed in a manner that allows the user to easily circumvent the system, thereby preventing the user to make alterations (col. 4, line 63 - col. 5, line 5). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Elazar et al. to encrypt the content key where the DRM component, i.e. buried nucleus, can decrypt the content key when it is delivered through a secure protocol and to decipher the encrypted key within the buried nucleus in order to make it inaccessible to an attacker. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Parks et al. suggest that sending the content key in encrypted form secures the key so that only that specific user device can obtain access to the digital content the user is authorized to access in col. 4, line 50 – col. 5, line 17 and col. 5, lines 35-42.

As per claim 11:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one LFSR (linear feedback shift register) (par. 25).

As per claim 12:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one reconfigurable

core (par. 27).

As per claim 13:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one programmable logic block (par. 27).

As per claim 14:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one non-volatile RAM (par. 27).

As per claim 15:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Furthermore, Elazar et al. teach wherein said buried nucleus includes at least one matrix multiplier (par. 34).

As per claim 16:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Not explicitly disclosed is wherein said encrypted key is encrypted with digital watermarking. However, Elazar et al. teach encrypting the actual content by adding overlay information. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Elazar et al. to also use digital watermarking to encrypt the key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Elazar et al. suggest there are several possible ways to encrypt a document which may be used in order to

secure and verify the contents which are encrypted in par. 36, lines 5-20.

As per claim 17:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Not explicitly disclosed is wherein said encrypted key is encrypted with a fast elliptical algorithm. However, Elazar et al. teach encrypting the actual content with a fast elliptical algorithm. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Elazar et al. to also use a fast elliptical algorithm to encrypt the key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Elazar et al. suggest there are several possible encryption algorithms which may be used in order to secure the contents being encrypted in par. 35.

As per claim 18:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Not explicitly disclosed is wherein said encrypted key is encrypted with Triple DES. However, Elazar et al. teach encrypting the actual content with Triple DES. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Elazar et al. to also use a Triple DES to encrypt the key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Elazar et al. suggest there are several possible encryption algorithms which may be used in order to secure the contents being encrypted in par. 35.

As per claim 19:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Not explicitly disclosed is wherein said encrypted key is encrypted with a Rijndael algorithm. However, Elazar et al. teach encrypting the actual content with AES. Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the method disclosed in Elazar et al. to also use a Rijndael algorithm to encrypt the key. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do so since Elazar et al. suggest there are several possible encryption algorithms which may be used in order to secure the contents being encrypted in par. 35.

As per claim 20:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Furthermore, Elazar et al. teach wherein said trusted authority is a back-end secure server (par. 33).

As per claim 21:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Furthermore, Elazar et al. teach wherein said trusted authority is a cell phone operator with a trusted command and control center (par. 29).

As per claim 22:

Elazar et al. and Parks et al. substantially teach the distributed architecture of claim 10. Furthermore, Elazar et al. teach wherein said trusted authority is an encrypted medium (par. 33).

**References Cited, Not Used*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

1. US Patent No. 6,449,367
2. US Pub. No. 2003/0226012
3. US Pub. No. 2003/0007646
4. US Pub. No. 2004/0054894
5. US Pub. No. 2003/0191942
6. US Pub. No. 2004/0064714
7. Dr. Dobb's| Rijndael: The Advanced Encryption Standard (cited to provide documentation suggesting that at least one matrix multiplier is inherent to AES)

The above references have been cited because they are relevant due to the manner in which the invention has been claimed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Nadia Khoshnoodi whose telephone number is (571) 272-3825. The examiner can normally be reached on M-F: 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Nadia Khoshnoodi/
Examiner, Art Unit 2137
8/29/2008

NK

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137